



Internal Audit Report

Third-Party Website Administration

TxDOT Internal Audit Division

Objective

To evaluate third-party website administration for consistency with Department of Information Resources (DIR) requirements, TxDOT branding, and compliance with state law.

Opinion

Based on the audit scope areas reviewed, control mechanisms require improvement and only partially address risk factors and exposures considered significant relative to impacting reporting reliability, operational execution, and compliance. The organization's system of internal controls requires improvement in order to provide reasonable assurance that key goals and objectives will be achieved. Significant improvements are required to correct control gaps and mitigate residual risk that may result in potentially significant negative impacts to the organization including the achievement of the organization's business/control objectives.

Overall Engagement Assessment		Needs Improvement		
Findings				
	Title	Control Design	Operating Effectiveness	Rating
Finding 1	Oversight and Management	X	X	Needs Improvement
Finding 2	Metric Reporting	X	X	Needs Improvement

Management concurs with the above findings and prepared management action plans to address deficiencies.

Control Environment

TxDOT.gov is the official public website for TxDOT. In situations where TxDOT.gov does not meet the desired needs, districts/divisions (D/Ds) can request approval from the Communications Division (CMD) to contract with an outside vendor for the creation of a third-party website to post information 1) for the public related to project planning, construction status, and planned route closures or 2) for internal TxDOT employees related to conferences. Texas Administrative Code, Chapter 215 requires that websites created for and/or maintained on behalf of TxDOT should be hosted on the Data Center Services (DCS) server environment unless otherwise approved by DIR.

CMD is required to be notified of third-party websites as they are responsible for TxDOT's internal and external communication functions and resources. Over time it was discovered that third-party websites were being developed and maintained by contracted external third-party vendors with contracts managed by the D/D and with the possibility of CMD not being notified. CMD public information officers (PIOs) across the state and D/D website coordinators are responsible for the monitoring of third-party website content. The same PIO and website coordinator oversight processes for third-party websites may vary based on location.

CMD has created web publishing procedures, web brand guidelines, and the Request for Exception (Form 2199) approval template to help ensure compliance with DIR and TxDOT requirements. In addition to the policies and procedures created by CMD, further direction

was communicated by the Chief Engineer and the Director of Communication and Customer Service on November 2017 to require 1) CMD approval before contracting website development work to an external vendor, and 2) adherence to TxDOT brand guidelines and approval by CMD before the website is published publicly.

Summary Results

Audit testing completed resulting in management action plans.

Finding	Scope Area	Evidence
1	<p>Website Development</p> <p>Website Operation</p> <p>Website Closure</p>	<p><u>Inventory</u> The third-party website listing maintained by CMD personnel was incomplete, with 19 more websites in place than inventoried.</p> <p><u>Compliance with State Law</u> A review of a judgmental sample of six third-party websites (created after November 2017) was completed to verify that content complied with requirements.</p> <ul style="list-style-type: none"> 6 of 6 (100%) websites did not include TxDOT's privacy policy or statement to describe practices used to protect personal identifying information (PII). <p>A review of all 32 active third-party websites identified and reported by CMD was completed to verify if DIR approval of websites not hosted on the DCS server was performed.</p> <ul style="list-style-type: none"> 31 of 32 (97%) websites did not reside on the DCS server, and did not have documentation to support DIR approval. <p><u>Compliance with TxDOT Requirements</u> A review of a judgmental sample of six third-party websites (created after November 2017) was completed to verify website creation approval, submission of estimated development and operation costs, and use of TxDOT's approved brand logo.</p> <ul style="list-style-type: none"> 6 of 6 (100%) websites did not have documentation to support CMD approval of website creation. 6 of 6 (100%) websites did not have estimated website costs submitted to CMD. 4 of 6 (67%) websites did not contain the approved brand logo. <p><u>Closure</u> A review of 44 third-party websites identified and reported by CMD was completed to verify if the project/event status (i.e., active, inactive) provided was accurate.</p> <ul style="list-style-type: none"> 4 of 44 (9%) websites with an inactive project status were still active. 12 of 44 (27%) websites with an active project status were inactive.

2	Website Operation	<p>A review of vendor-provided third-party website metric reporting for a judgmental sample of six websites (created after November 2017) was completed to verify monitoring of third-party website performance.</p> <ul style="list-style-type: none"> • 3 of 6 (50%) D/Ds did not obtain reporting from the vendor. • 3 of 6 (50%) D/Ds obtained reporting from vendor but did not submit the reporting to CMD – Web Services Branch.
---	-------------------	---

Audit testing completed not resulting in management action plans.

Scope Area	Evidence
Website Development	<p>A review of the executed contracts for a judgmental sample of six third-party websites (created after November 2017) was completed to verify contract language was compliant with DIR and TxDOT website standard requirements.</p> <ul style="list-style-type: none"> • 6 of 6 (100%) executed third-party contracts contained requirements for the vendor to follow DIR Security Controls Standard Catalog, TAC Chapter 206 – State Websites, and TxDOT logo requirements.

Audit Scope and Methodology

The audit was conducted during the period from September 30, 2019 to November 22, 2019. Testing focused on the development, operation, and closure of third-party websites developed and maintained by vendors on behalf of TxDOT.

Scope Area 1: Website Development – evaluation of third-party website development in compliance with state law, as well as, DIR and TxDOT brand guidelines, policy, and procedures.

Methodology included:

- Compared listings containing 56 websites compiled by CMD's four PIO sections and Creative Services Section to verify third-party website inventory completeness.
- Verified a total of 44 third-party websites from the CMD listings and selected a judgmental sample of six based on project/event type and creation date.
- Reviewed e-mail documentation and/or Form 2199 to support CMD approval of third-party website development and compliance with state law, DIR requirements, and TxDOT brand guidelines for the six sampled websites.
- Determined the host server location for 32 active third-party websites identified by CMD using three websites: 1) Hosting Checker (<https://hostingchecker.com>), 2) WHOIS IP Lookup Tool (<https://www.ultratools.com/tools/ipWhoisLookupResult>), 3) Dig Web Interface (<https://digwebinterface.com/>), and verified DIR approval was obtained for websites not hosted on the DCS server.

Scope Area 2: Website Operation – evaluation of third-party website operation and monitoring.

Methodology included:

- Reviewed metric reporting obtained from the vendor for the six judgmentally sampled third-party websites to verify receipt by responsible D/D and CMD – Web Services Branch.

Scope Area 3: Website Closure – assessment of third-party website closure at completion of the project.

Methodology included:

- Reviewed 44 third-party websites compiled by CMD to determine if the project/event status (i.e., active, inactive) provided within the listing were accurate.
- Followed up with the responsible D/D to determine if websites identified by CMD as inactive and found to be active were still in use.

Methodology included within Scope 1, Scope 2, and Scope 3:

- Reviewed state guidance that included Texas Administrative Code and DIR requirements.
- Reviewed internal TxDOT policies and procedures that included the Web Publishing Policies and Procedures and TxDOT Brand Guidelines.
- Interviewed CMD Director, Creative Services Section Director, PIOs, project managers, and D/D web coordinators.
- Reviewed the executed contracts for the judgmental sample of six third-party websites to verify contract language complied with DIR and TxDOT website standard requirements and the amount allocated for website development and operation.
- Reviewed invoices for the judgmental sample of six third-party websites to evaluate costs associated with website development and operation.

Background

This report is prepared for the Texas Transportation Commission and for the Administration and Management of TxDOT. The report presents the results of the Third-Party Website Administration audit which was conducted as part of the Fiscal Year (FY) 2020 Audit Plan.

Review and coordination of vendor-developed websites for compliance with DIR requirements and the TxDOT branding is to be performed by CMD's Creative Services Section, as well as, PIOs grouped into four sections by district location: Southwest, Southeast, Northwest, and Northeast. Website structure and content availability support is provided by CMD's Web Services Branch who works in coordination with the Information Technology Division (ITD) to ensure website content is accessible.

In addition to the PIOs located within the districts, each D/D is responsible for appointing a website coordinator to work with CMD for internal and external website management. Per the Web Publishing Policies and Procedures, both the responsible D/D and CMD have a responsibility to ensure website content follows state and TxDOT guidelines prior to and during website operation.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards and in conformance with the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Recommendations to mitigate risks identified were provided to management during the engagement to assist in the formulation of the management action plans included in this report. The Internal Audit Division uses the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework version 2013.

A defined set of control objectives was utilized to focus on reporting, operational, and compliance goals for the identified scope areas. Our audit opinion is an assessment of the health of the overall control environment based on (1) the effectiveness of the enterprise risk management activities throughout the audit period and (2) the degree to which the defined control objectives were being met. Our audit opinion is not a guarantee against reporting misstatement and reliability, operational sub-optimization, or non-compliance, particularly in areas not included in the scope of this audit.

Detailed Findings and Management Action Plans (MAP)

Finding No. 1: Oversight and Management

Condition

Third-party websites were not in conformance with state law, Department of Information Resources (DIR) requirements, or internal requirements and guidelines. Oversight and management activities being performed did not occur to help ensure required performance, and costs associated with third-party websites.

Effect/Potential Impact

Without proper oversight and management of third-party websites:

- Districts and divisions (D/Ds) cannot monitor all site content for accuracy, relevance, and adherence to applicable requirements.
- Outdated or inaccurate information may be conveyed to the public visiting the site.
- Additional time could be spent by TxDOT personnel to respond to inquiries from the public on content or sites that are not known to exist.

Websites not hosted on a secure server environment such as Data Center Services (DCS) server environment could increase the susceptibility of hacking, loss of data, reporting of incorrect information, and the spread of malware. In addition, contracts that are executed without the inclusion of website requirements can impede D/D and/or Communications Division's (CMD) enforcement of the vendors' agreements.

Without a cost-benefit analysis component or procedures to monitor cost impacts of websites, the responsible district/division or CMD would not have all the necessary information to determine whether creation of a third-party website is in the best interest of TxDOT or if it should remain in-house.

Criteria

Texas Administrative Code (TAC), §215.10 requires agencies requesting exemption from all or part of DCS to obtain approval from the Director of the DCS Program.

TAC §206.52 states that each state agency must publish a privacy notice describing applicable provisions of its privacy policy on the home page of each website. The privacy notice should include practices employed to protect personal identifying information (PII).

TxDOT's Web Publishing Processes and Procedures and TxDOT Brand Guidelines outlines:

- Approval from CMD must be obtained for exceptions authorizing the creation of a website separate from TxDOT.gov.
- The owning D/D must provide an estimate of the cost of contracting, designing, and maintaining the website prior to the site's development. The costs can be based on the average of other similar project costs.
- Websites, unless otherwise authorized, will reside on the state DCS server platform as required by state law.
- Guidelines applying to TxDOT.gov and those sites maintained by third parties or vendors on behalf of TxDOT.

- The D/D is responsible for ensuring the website is updated with new and relevant information for the duration the website is active.
- D/Ds must review website content at least quarterly.
 - CMD is responsible for initiating the quarterly content reviews.
- Use of brand guidelines for website content to include an approved version of the TxDOT logo with the proper markings ® or ™.
- TxDOT privacy policy must be posted on the website homepage.
- Description of practices used to protect PII by TxDOT.

Cause

CMD has not established a method to fully identify and confirm the completeness and accuracy of third-party website inventory and host server location. In addition, CMD has not established policies and procedures for the closure of third-party websites.

The Request for Exception (Form 2199) approval template does not include fields to capture the estimated costs associated with third-party website development and operation.

Districts/Divisions did not obtain CMD approval prior to contracting website development work to an external vendor. CMD did not obtain or retain DIR approval for third-party websites not hosted on the DCS server. In addition, CMD does not review third-party website content for adherence to state laws and TxDOT brand guidelines prior to the website activation.

Quarterly content reviews of third-party websites are not initiated by CMD nor performed by the responsible D/D. Employees involved in the planning, development, and operation of third-party websites were unaware of the roles and responsibilities required by state, DIR, and internal TxDOT policy. Periodic reviews of third-party website content and activity were also not performed by CMD.

Evidence

Inventory

Third-party websites provided by 1) CMD - Creative Services Section, as of August 2019, and 2) PIOs within CMD's four PIO sections, as of October 2019, were compared and identified a total of 56 websites.

- 19 of 56 (34%) websites were identified as additional third-party websites not included within the initial list provide by CMD – Creative Services Section who should have an awareness of all such websites.
- 12 of 56 (21%) websites, as identified by CMD and PIO sections, were assessed and determined to be non-third-party websites.

Compliance with State Law

A judgmental selection of six third-party websites created after November 2017 was reviewed to verify if the content contained within the website was compliant with DIR privacy policy and PII requirements.

- 6 of 6 (100%) websites did not include TxDOT's privacy policy.
- 6 of 6 (100%) websites did not include a statement to describe practices used by TxDOT to protect PII.

A review of 32 confirmed active third-party websites identified by CMD was performed to determine the host server location and verify if DIR exception approval was obtained for any websites not hosted on the DCS server.

- 31 of 32 (97%) websites did not reside on the DCS server and did not have documentation that could be provided by CMD or Information Technology Division to support DIR exception approval.

Compliance with TxDOT Requirements

A judgmental selection of six third-party websites created after November 2017 was reviewed to verify if CMD approval was obtained for the 1) creation of third-party websites, 2) submission of estimated costs for the contracting, design, and operation of the website prior to development, and 3) inclusion of TxDOT's approved brand logo on the website.

- 6 of 6 (100%) websites did not have documentation to support pre-approval by CMD.
- 6 of 6 (100%) websites did not have documentation submitted to CMD outlining estimated costs for the website.
 - In addition, actual costs associated with website development and operation could not be provided by CMD or the responsible D/D.
- 4 of 6 (67%) were noncompliant with TxDOT logo requirements.
 - One did not contain the TxDOT logo on the website at all.
 - Two had logos that included colors that did not meet brand guidelines.
 - One had a logo that included formatting that did not meet brand guidelines.

Closure

A review of 44 third-party websites compiled by CMD was performed to determine if the project/event status provided by CMD was accurate.

- 4 of 44 (9%) websites with an inactive project status were still active.
- 12 of 44 (27%) websites with an active project status were inactive.

Management Action Plan (MAP):

MAP Owner: Michael Sledge, Creative Services Section Director, Communications Division

MAP 1.1: The Communications Division (CMD) will:

- Revise Form 2199 to include:
 - A field to capture the estimated cost for developing and maintaining the website requested.
 - Information on how to estimate the cost for developing and maintaining the third-party website that is being requested, and information regarding the reasonable cost of developing and maintaining the website.
 - A field to capture the host server location for the third-party website being requested.
 - Information about the Department of Information Resources rules concerning hosting website domains for websites created for and/or maintained on behalf of TxDOT.
 - A checklist of criteria that must be met before creating a third-party website, and before a third-party website can be approved to go live.
 - A field to capture CMD's review and approval for the website to go live.

- Revise the Web Publishing Processes and Procedures to include:
 - The method established in MAP 1.2 to maintain a complete list of third-party websites.
 - Responsibility of district and divisions to ensure updates to the third-party website primary contacts are provided to the Communications Division (CMD).
 - Guidelines and timelines developed in MAP 1.2 for content review by the districts, divisions, and CMD to ensure website compliance with state law and TxDOT branding guidelines.
 - Procedures for websites not in compliance and the escalation process to bring them into compliance.
 - Requirements for mandatory training on third-party website governance and administration for TxDOT district and division staff and vendors involved in the third-party website process.
 - Process and procedures on closure of third-party websites that are no longer needed.

Completion Date: February 15, 2020

MAP 1.2: The Communications Division will:

- Utilize Form 2199 to identify and maintain a list of third-party websites that will include the host server location for each website.
- Maintain a list of the district and division primary contact for questions or comments regarding third-party websites.
- Develop guidelines and timelines to monitor and review website content by the districts, divisions and the Communications Division to ensure website compliance with state law and TxDOT branding guidelines. The guidelines will include best practices for the quarterly review of third-party websites.

Completion Date: March 15, 2020

MAP 1.3: The Communications Division will:

- Collaborate with appropriate divisions to develop and provide training on third-party website governance and administration for TxDOT district and division staff, and vendors involved in the third-party website process that will include all the revisions and guidelines stated in MAP 1.1, and MAP 1.2.
- Determine the training method of delivery (i.e., in person, WebEx) and frequency (i.e., as needed, quarterly, semi-annually) in which the training will be conducted by CMD based on budgetary approval.
- Work with the Information Technology Division to determine the impact on staffing and request the additional resources required to meet the need of providing review, approval, training, and guidance for the more than 50 third-party websites and future websites.

Completion Date: April 15, 2020

Finding No. 2: Metric Reporting**Condition**

Responsible districts/divisions (D/Ds) did not always obtain nor provide metric reporting of third-party websites to Communications Division (CMD) - Web Services Branch for further monitoring/validation of website performance and/or updates.

Effect/Potential Impact

Without third-party website metric monitoring and reporting, CMD - Web Services Branch does not have the ability to manage website audience, traffic, content, and timeliness of updates.

Criteria

TxDOT's Web Publishing Processes and Procedures require third-party website metric reporting be provided at least quarterly as determined by the applicable D/D. The metric report should also be provided to CMD - Web Services Branch for review.

Cause

The third-party contracts reviewed did not include specific requirements that metric reporting be provided by the third-party vendor. D/D personnel were not aware of the requirements to obtain metric reporting from the vendor. In addition, monitoring of the metric reporting submissions was not performed by CMD as the metric information was either not obtained nor passed along for their review.

Evidence

Interviews and review of documentation to support metric reporting for third-party websites was performed for a judgmental sample of six websites (created after November 2017) from six D/Ds.

- 3 of 6 (50%) D/Ds did not obtain metric reporting from the third-party vendor.
- 3 of 6 (50%) D/Ds obtained metric reporting from the vendor, but did not submit the reporting to CMD - Web Services Branch for monitoring.

Management Action Plan (MAP):

MAP Owner: Michael Sledge, Creative Services Section Director, Communications Division

MAP 2.1: The Web Publishing Processes and Procedures will be revised to include:

- Communications Division review of contracts including third-party website development and maintenance prior to contract execution.
- The metric reporting processes and procedures developed as part of MAP 2.2.
- Information on website metrics reporting, explaining in detail reporting requirements, when reports are due and to whom. The process will also cover what to do when vendors fail to provide metrics reports to TxDOT and how to ensure and confirm compliance.

Completion Date: February 15, 2020

MAP 2.2: The Communications Division will:

- Work with the Contract Services Division to ensure language is included within the contract templates regarding conformance with state law, Department of Information Resources (DIR) requirements, and TxDOT policy and procedures, and brand guidelines for websites created for and/or maintained on behalf of TxDOT.
- Work with the districts and divisions to develop processes and procedures for the reporting of consistent third-party website metrics by the external vendor to TxDOT.
- Communicate the revisions made to the Web Publishing Processes and Procedures as defined in MAP 2.1 to applicable division and district personnel involved in the third-party website process.

Completion Date: April 15, 2020

Summary Results Based on Enterprise Risk Management Framework

Audit Results Dashboard				
Third-Party Website Administration				
Business Objectives (Reporting, Operational, Compliance)		Scope Areas Evaluated		
		R, O, C	R, O, C	O, C
ERM Component	Control Activities	Website Development	Website Operation	Website Closure
Control Environment	Organizational Tone	1	1, 2	1
	Business Objective/Goal-Setting			
	Resource Capacity	1	1	
	Forecasting/Budget			
	Training and Development			
Risk Assessment	Risk Identification/Planning			
	Risk Assessment/Impact Analysis			
	Risk Response/Cost-Benefit Analysis	1		
	Business Continuity			
Control Activities	Policies/Procedure Development & Maintenance	1		1
	Approvals/Authorizations	1		
	Supporting Evidence/Records Retention	1	2	
	Segregation of Duties/System Access			
	Safeguarding Assets/Security			
Information & Communication	Information Classification			
	Information Input			
	Information Processing			
	Information Output			
	Internal and External Reporting	1		
Monitoring	Exception Reporting Review			
	Reconciliations			
	Root-Cause Analysis			
	Evaluations/Inspections	1	1, 2	1
	Management Action Plans			
Scope Area Assessment				
Rating Assessment Grid		Exemplary	Satisfactory	Needs Improvement
				Unsatisfactory

Closing Comments

The results of this audit were discussed with the Communications Division Creative Services Section Director and provided to the Communications Division Director on December 3, 2019. The Internal Audit Division appreciates the cooperation and assistance received from the personnel contacted during this audit.